Installation et configuration de Fail2ban

1 - Prérequis

Téléchargement des paquets nécessaires au fonctionnement de Fail2ban

```
apt install fail2ban iptables -y
```

2 - Configuration

Configuration de fail2ban

```
nano /etc/fail2ban/jail.conf
# Réseau qui ne sera pas pris en compte par Fail2ban
ignoreip = <Réseau1> <Réseau2>

# Temps pendant lequel l'hôte sera banni
bantime = <TempsEnSecondes>
findtime = <TempsEnSecondes>

# Tentatives maximales
maxretry = <1-9999>

# Activation de Fail2ban pour SSH
[sshd]
enabled = true
```

Théo PERDIGON

3 - Commandes d'utilisation de Fail2ban

Lister toutes les commandes du Client

```
fail2ban-client -h
```

Afficher l'état du serveur

```
fail2ban-client status
```

Vérification du statut de SSHD

```
fail2ban-client status sshd
```

Bannir une IP

```
fail2ban-client set sshd banip <IP>
```

Débannir une IP

```
fail2ban-client set sshd unbanip <IP>
```

Visualisation des logs

```
tail -f /var/log/syslog
tail -f /var/log/fail2ban.log
```

Redémarrer le service Fail2ban

```
systemctl restart fail2ban.service
```